FULL VERSION OF PENDING CLAIMS

1   1.   (Currently Amended) A cryptographic apparatus comprising:

2   a data reading means for reading content data and cryptographic information from

3   a portable storage medium, the cryptographic information including information used to specify

4   a certain part of the content data on which cryptographic processing is to be performed;

5   a part specifying means for specifying, based on the read cryptographic

6   information, the certain part of the read content data at least by searching for a specific data

7   section in the read content data; and

8   a cryptographic processing means for performing one of encryption and

9   decryption on the certain part of the read content data.

1   2.   (Original) The cryptographic apparatus of Claim 1, wherein:

2   a plurality of pieces of content data are each recorded as a file on the storage

3   medium, along with cryptographic information for each of a plurality of file types; and

4   the data reading means reads, from the storage medium, the

5   content data of a file and the cryptographic information for a corresponding file

6   type.

1   3.   (Original) The cryptographic apparatus of Claim 2, wherein:

2   the cryptographic information includes a reference instruction indicating that a

3   data section in the content data be referred to, and

4   the part specifying means specifies the certain part by referring to the data section

5   as indicated by the reference instruction.

1   4.   (Original) The cryptographic apparatus of Claim 3, wherein:

2   the cryptographic information includes bit pattern information showing a certain

3   bit sequence; and

4   the part specifying means detects, in the content data, bit data that matches the bit

5   sequence shown in the bit pattern information, and uses a location of the bit data as a basis for

6   specifying the certain part, the certain part having a fixed positional relationship to the bit data.

1   5.   (Original) The cryptographic apparatus of Claim 4, wherein:

2   the indicated data section shows a length of the certain part; and

3   the part specifying means specifies the certain part of the content data by referring

4   to the data section as indicated by the reference instruction, and calculating the length of the

5   certain part based on the referenced data section.

1   6.   (Original) The cryptographic apparatus of Claim 5, wherein:

2   the cryptographic information includes a value showing a unit used for the

3   indicated data section; and

4   the part specifying means specifies the certain part by multiplying the length

5   shown by the data section with the unit value to calculate the length of the certain part.

1   7.   (Currently Amended) The cryptographic apparatus of Claim 6, wherein:

2   the cryptographic information further includes a detect instruction for detecting,

3 from the content data, bit data that matches the certain bit sequence shown by the bit pattern

4 information, and specifies ~~determines~~ the order in which the reference and detect instructions are

5 performed; and

6   the part specifying means specifies the certain part in the content data by

7 performing, in the ~~predetermined~~ order specified by the cryptographic information, operations

8 indicated by each of the instructions.

1   8.   (Original) The cryptographic apparatus of Claim 3, wherein:

2   the cryptographic information further includes at least one piece of algorithm

3 information for specifying an algorithm used for cryptographic processing; and

4   the cryptographic processing means performs one of encryption and decryption on

5 the certain part using the specified algorithm.

1   9.   (Original) The cryptographic apparatus of Claim 2, wherein:

2   the cryptographic information further includes at least one piece of algorithm

3 information for specifying an algorithm used for cryptographic processing; and

4   the cryptographic processing means performs one of encryption and decryption on

5 the certain part using the specified algorithm.

1   10.   (Original) The cryptographic apparatus of Claim 1, wherein

2   the cryptographic information includes a reference instruction indicating that a

3   data section in the content data be referred to, and

4   the part specifying means specifies the certain part by referring to the data section

5   as indicated by the reference instruction.

1   11.   (Original) The cryptographic apparatus of Claim 10, wherein:

2   the cryptographic processing means encrypts the certain part; and

3   the cryptographic apparatus further comprises a content data recording means for

4   recording the encrypted content data onto the storage medium.

1   12.   (Original) The cryptographic apparatus of Claim 10, wherein:

2   the cryptographic processing means decrypts the certain part of the content data;

3   and

4   the cryptographic apparatus further comprises:

5   an encrypting information reading means for reading, from another portable

6   storage medium, encrypting information including information used to specify a certain part in

7   the decrypted content data to be encrypted;

8   an encryption part specifying means for specifying a certain part to be encrypted

9   in the decrypted content data, according to the encrypting information;

10   an encrypting means for encrypting the part specified by the encrypting

11   information; and

12   a content data recording means for recording the encrypted content data onto the

13   other storage medium.

1   13.   (Original) The cryptographic apparatus of Claim 1, wherein:

2   the cryptographic information further includes at least one piece of algorithm

3   information for specifying an algorithm used for cryptographic processing; and

4   the cryptographic processing means performs one of encryption and decryption on

5   the certain part using the specified algorithm.

1   14.   (Original) The cryptographic apparatus of Claim 13, wherein:

2   the cryptographic information includes a plurality of pieces of algorithm

3   information, and pieces of range information each showing a range over which an algorithm is

4   applied; and

5   the cryptographic processing means selects, for each application range in the

6   certain part, a piece of algorithm information based on the range information, and uses an

7   algorithm specified by the piece of algorithm information to perform one of encryption and

8   decryption on the application range.

1   15.   (Original) The cryptographic apparatus of Claim 14, wherein:

2   the cryptographic information includes information showing priority ratings

3   indicating an order in which the pieces of algorithm information should be applied; and

4   when the application ranges of a plurality of algorithms overlap, the cryptographic

5   processing means selects pieces of algorithm information according to the priority ratings.

1   16.   (Original) The cryptographic apparatus of Claim 1, wherein:

2   the cryptographic processing means encrypts the certain part; and

3   the cryptographic apparatus further comprises a content data recording means for

4   recording the encrypted content data onto the storage medium.

1   17.   (Original) The cryptographic apparatus of Claim 1, wherein:

2   the cryptographic processing means decrypts the certain part.

1   18.   (Original) The cryptographic apparatus of Claim 17, further comprising:

2   an encrypting information reading means for reading, from another portable

3   storage medium, encrypting information including information used to specify a certain part in

4   the decrypted content data to be encrypted;

5   an encryption part specifying means for specifying a certain part to be encrypted

6   in the decrypted content data according to the encrypting information;

7   an encrypting means for encrypting the part specified by the encrypting

8   information; and

9   a content data recording means for recording the encrypted content data onto the

10   other storage medium.

1   19.   (Currently Amended) A cryptographic apparatus encrypting content data and

2   recording the encrypted data onto a storage medium, the cryptographic apparatus comprising:

3   a content data obtaining means for obtaining content data;

4   a cryptographic information reading means for reading, from a portable storage

5   medium, cryptographic information including information used to specify a certain part of the

6   content data on which cryptographic processing is to be performed;

7   a part specifying means for specifying the certain part of the obtained content data

8   based on the read cryptographic information at least by searching for a specific data section in

9   the obtained content data;

10   a cryptographic processing means for encrypting the certain part; and

11   a content data recording means for recording the encrypted content data onto the

12   storage medium.

1   20.   (Original) The cryptographic apparatus of Claim 19, wherein:

2   the storage medium stores a plurality of pieces of content data as files, along with

3   cryptographic information for a plurality of file types corresponding to files that can be stored on

4   the storage medium; and

5   the cryptographic information reading means reads the cryptographic information

6   for a file type from the storage medium; and

7   the content data recording means records the encrypted content data onto the

8   storage medium as a file of the file type corresponding to the read cryptographic information.

1   21.   (Original) The cryptographic apparatus of Claim 20, wherein:

2   the cryptographic information includes bit pattern information showing a certain

3 bit sequence; and

4   the part specifying means detects, in the content data, bit data that matches the bit

5 sequence shown in the bit pattern information, and uses a location of the bit data as a basis for

6 specifying the certain part, the certain part having a fixed positional relationship to the bit data.

1   22.   (Original) The cryptographic apparatus of Claim 21, wherein:

2   the cryptographic information includes a reference instruction indicating that a

3 data section in the content data be referred to, the data section showing a length of the certain

4 part; and

5   the part specifying means specifies the certain part by referring to the data section

6 as indicated by the reference instruction and calculating the length of the certain part based on

7 the referenced data section.

1   23.   (Original) The cryptographic apparatus of Claim 21, wherein:

2   the cryptographic information further includes at least one piece of algorithm

3 information specifying an algorithm used for cryptographic processing; and

4   the cryptographic processing means encrypts the certain part using the algorithm

5 specified by the algorithm information.

1   24.   (Original) The cryptographic apparatus of Claim 19, wherein:

2   the cryptographic information includes bit pattern information showing a certain

3   bit sequence; and

4   the part specifying means detects, in the content data, bit data that matches the bit

5   sequence shown in the bit pattern information, and uses a location of the bit data as a basis for

6   specifying the certain part, the certain part having a fixed positional relationship to the bit data.

1   25.   (Original) The cryptographic apparatus of Claim 24, wherein:

2   the cryptographic information includes a reference instruction indicating that a

3   data section in the content data be referred to, the data section showing a length of the certain

4   part; and

5   the part specifying means specifies the certain part by referring to the data section

6   as indicated by the reference instruction and calculating the length of the certain part based on

7   the referenced data section.

1   26.   (Original) The cryptographic apparatus of Claim 19, wherein:

2   the cryptographic information further includes at least one piece of algorithm

3   information specifying an algorithm used for cryptographic processing; and

4   the cryptographic processing means encrypts the certain part using the algorithm

5   specified by the algorithm information.

1   27.   (Original) The cryptographic apparatus of Claim 26, wherein:

2   the cryptographic information includes a plurality of

3   pieces of algorithm information and pieces of range information each showing a

4   range in the content data over which an algorithm is applied; and

5   the cryptographic processing means selects, for each application range in the

6   certain part, a piece of algorithm information based on the range information, and uses an

7   algorithm specified by the piece of algorithm information to encrypt data in the application

8   range.

1   28.   (Original) The cryptographic apparatus of Claim 27, wherein:

2   the cryptographic information includes information showing priority ratings

3   indicating an order in which the pieces of algorithm information should be applied; and

4   when the application ranges of a plurality of algorithms overlap, the cryptographic

5   processing means selects pieces of algorithm information according to the priority ratings.

1   29.   (Currently Amended) A cryptographic apparatus comprising:

2   a data obtaining means for obtaining, from received data, content data, and

3   cryptographic information including information used to specify a certain part of the content data

4   on which cryptographic processing is to be performed, the received data consisting of content

5   data and cryptographic information that has been multiplexed and transmitted;

6   a part specifying means for specifying the certain part of the obtained content data

7   based on the obtained cryptographic information at least by searching for a specific data section

8   in the obtained content data; and

9   a cryptographic processing means for performing one of encryption and

10   decryption on the certain part of the content data.

1   30.   (Original) The cryptographic apparatus of Claim 29, wherein:

2   the cryptographic information includes a reference instruction indicating that a

3   data section in the content data be referred to, and

4   the part specifying means specifies the certain part by referring to the data section

5   as indicated by the reference instruction.

1   31.   (Original) The cryptographic apparatus of Claim 30, wherein:

2   the cryptographic information includes sync pattern information showing a certain

3   bit sequence; and

4   the part specifying means detects, in the content data, a sync pattern

5   corresponding to the bit sequence shown in the sync pattern information, and uses a location of

6   the sync pattern as a basis for specifying the certain part, the certain part having a fixed

7   positional relationship to the sync pattern.

1   32.   (Original) The cryptographic apparatus of Claim 31, wherein:

2   the part specifying means verifies the authenticity of the detected sync pattern by

3   checking whether another sync pattern is located at a position a set interval away from the

4   location of the detected sync pattern.

1 33. (Currently Amended) The cryptographic apparatus of Claim 31, wherein:

2 the cryptographic information further includes flag pattern information showing a

3 bit sequence, which is not the certain bit sequence shown by the sync pattern information, and

4 position information specifying the position of the bit sequence; and

5 the part specifying means verifies whether the bit sequence shown by the flag

6 pattern information exists at the position in the content data specified by the position

7 information.

1 34. (Original) The cryptographic apparatus of Claim 31, wherein:

2 the indicated data section shows a length of the certain part; and

3 the part specifying means specifies the certain part of the content data by referring

4 to the data section as indicated by the reference instruction, and calculating the length of the

5 certain part based on the referenced data section.

1 35. (Original) The cryptographic apparatus of Claim 34, wherein:

2 the cryptographic information includes a value showing a unit used for the

3 indicated data section; and

4 the part specifying means specifies the certain part by multiplying the length

5 shown by the data section with the unit value to calculate the length of the certain part.

1   36.   (Currently Amended) The cryptographic apparatus of Claim 35, wherein:

2   the cryptographic information further includes a detect instruction for detecting,

3   from the content data, bit data that matches the certain bit sequence shown by the bit pattern

4   information, and <u>specifies</u> ~~determines~~ the order in which the reference and detect instructions are

5   performed; and

6   the part specifying means specifies the certain part in the content data by

7   performing, in the ~~predetermined~~ order <u>specified by the cryptographic information,</u> operations

8   indicated by each of the instructions.

1   37.   (Original) The cryptographic apparatus of Claim 31,

2   the cryptographic information further includes at least one piece of algorithm

3   information for specifying an algorithm used for cryptographic processing; and

4   the cryptographic processing means performs one of encryption and decryption on

5   the certain part using the specified algorithm.

1   38.   (Currently Amended) The cryptographic apparatus of Claim 29, wherein:

2   the cryptographic information further includes at least one piece of algorithm

3   information for specifying an algorithm used for cryptographic processing; and

4   the cryptographic processing means performs one of encryption and decryption on

5   the certain part using the specified <u>algorithm.</u>

1   39.   (Original) The cryptographic apparatus of Claim 38, wherein:

2   the cryptographic information includes a plurality of pieces of algorithm

3   information, and pieces of range information each showing a range over which an algorithm is

4   applied; and

5   the cryptographic processing means selects, for each application range in the

6   certain part, a piece of algorithm information based on the range information, and uses an

7   algorithm specified by the piece of algorithm information to perform one of encryption and

8   decryption on the application range.

1   40.   (Original) The cryptographic apparatus of Claim 39, wherein:

2   the cryptographic information includes information showing priority ratings

3   indicating an order in which the pieces of algorithm information should be applied; and

4   when the application ranges of a plurality of algorithms overlap, the cryptographic

5   processing means selects pieces of algorithm information according to the priority ratings.

1   41.   (Original) The cryptographic apparatus of Claim 29,

2   the cryptographic processing means decrypts the certain part.

1   42.   (Currently Amended) A cryptographic apparatus performing cryptographic

2   processing on content data, the cryptographic apparatus comprising:

3   a content data obtaining means for obtaining content data;

4   a cryptographic information obtaining means for obtaining cryptographic

5   information including information specifying a part on which cryptographic processing is to be

6   performed in the contents data, the information including a reference instruction indicating that a

7   data section in the content data be referred to;

8   a part specifying means for specifying the certain part of the content data based on

9   the cryptographic information by <u>searching for and</u> referring to the data section in the content

10   data as indicated by the reference instruction; and

11   a cryptographic processing means for performing one of encryption and

12   decryption on the certain part.

1   43.   (Original) The cryptographic apparatus of Claim 42, wherein:

2   the cryptographic information includes bit pattern information showing a certain

3   bit sequence; and

4   the part specifying means detects, in the content data, bit data that matches the bit

5   sequence shown in the bit pattern information, and uses a location of the bit data as a basis for

6   specifying the certain part, the certain part having a fixed positional relationship to the bit data.

1   44.   (Original) The cryptographic apparatus of Claim 43, wherein:

2   the cryptographic information includes a reference instruction indicating that a

3   data section in the content data be referred to, the data section showing a length of the certain

4   part; and

5   the part specifying means specifies the certain part by referring to the data section

6   as indicated by the reference instruction and calculating the length of the certain part based on

7   the referenced data section.

1   45.   (Original) The cryptographic apparatus of Claim 44, wherein:

2   the cryptographic information includes a value showing a unit used for the

3   indicated data section; and

4   the part specifying means specifies the certain part by multiplying the length

5   shown by the data section with the unit value to calculate the length of the certain part.

1   46.   (Currently Amended) The cryptographic apparatus of Claim 45, wherein:

2   the cryptographic information further includes a detect instruction for detecting,

3   from the content data, bit data that matches the certain bit sequence shown by the bit pattern

4   information, and <u>specifies</u> ~~determines~~ the order in which the reference and detect instructions are

5   performed; and

6   the part specifying means specifies the certain part in the content data by

7   performing, in the ~~predetermined~~ order <u>specified by the cryptographic information</u>, operations

8   indicated by each of the instructions.

1   47.   (Original) The cryptographic apparatus of Claim 42, wherein:

2   the cryptographic information further includes at least one

3   piece of algorithm information for specifying an algorithm used for cryptographic

4   processing; and

5   the cryptographic processing means performs one of encryption and decryption on

6   the certain part using the specified algorithm.

1   48.   (Original) The cryptographic apparatus of Claim 47, wherein:

2   the cryptographic information includes a plurality of pieces of algorithm

3   information, and pieces of range information each showing a range over which an algorithm is

4   applied; and

5   the cryptographic processing means selects, for each application range in the

6   certain part, a piece of algorithm information based on the range information, and uses an

7   algorithm specified by the piece of algorithm information to perform one of encryption and

8   decryption on the application range.

1   49.   (Original) The cryptographic apparatus of Claim 48, wherein:

2   the cryptographic information includes information showing priority ratings

3   indicating an order in which the pieces of algorithm information should be applied; and

4   when the application ranges of a plurality of algorithms overlap, the cryptographic

5   processing means selects pieces of algorithm information according to the priority ratings.

1   50.   (Original) The cryptographic apparatus of Claim 42, wherein:

2   the cryptographic processing means encrypts the certain part of the content data;

3   and

4   the cryptographic apparatus further comprises a multiplexing transmission means

5   for multiplexing the encrypted content data and the cryptographic information and transmitting

6   the multiplexed data.

1   51.   (Currently Amended) A program recording medium storing a control program for

2   having a computer execute cryptographic processing on content data, the control program

3   comprising:

4   a data reading step for reading content data and cryptographic information from a

5   portable storage medium, the cryptographic information including information used to specify a

6   certain part of the content data on which cryptographic processing is to be performed;

7   a part specifying step for specifying, based on the read cryptographic information,

8   the certain part of the read content data at least by searching for a specific data section in the read

9   content data; and

10   a cryptographic processing step for performing one of encryption and decryption

11   on the certain part of the read content data.

1   52.   (Original) The program recording medium of Claim 51, wherein:

2   a plurality of pieces of content data are each recorded as a file on the storage

3   medium, along with cryptographic information for each of a plurality of file types; and

4   the data reading step reads, from the storage medium, the content data of a file

5   and the cryptographic information for a corresponding file type.

1   53.   (Original) The program recording medium of Claim 51, wherein:

2   the cryptographic information includes bit pattern information showing a certain

3 bit sequence; and

4   the part specifying step detects, in the content data, bit data that matches the bit

5 sequence shown in the bit pattern information, and uses a location of the bit data as a basis for

6 specifying the certain part, the certain part having a fixed positional relationship to the bit data.

1   54.   (Original) The program recording medium of Claim 51, wherein:

2   the cryptographic information further includes at least one piece of algorithm

3 information for specifying an algorithm used for cryptographic processing; and

4   the cryptographic processing step performs one of encryption and decryption on

5 the certain part using the specified algorithm.

1   55.   (Original) The program recording medium of Claim 51, wherein:

2   the cryptographic processing step encrypts the certain part; and

3   the cryptographic processing further comprises a content data recording step for

4 recording the encrypted content data onto the storage medium.

1   56.   (Original) The program recording medium of Claim 51, wherein:

2   the cryptographic processing step decrypts the certain part.

1   57.   (Original) The program recording medium of Claim 56, wherein the

2   cryptographic processing further comprises:

3   an encrypting information reading step for reading, from another portable storage

4   medium, encrypting information including information used to specify a certain part in the

5   decrypted content data to be encrypted;

6   an encryption part specifying step for specifying a certain part to be encrypted in

7   the decrypted content data, according to the encrypting information;

8   an encrypting step for encrypting the part specified by the encrypting information;

9   and

10   a content data recording step for recording the encrypted content data onto the

11   other storage medium.

1   58.   (Currently Amended) A program recording medium storing a control program for

2   having a computer storing content data execute cryptographic processing on the content data, the

3   cryptographic processing (1) including encryption of the content data and recording of the

4   encrypted content data onto a storage medium, and (2) comprising the following steps:

5   a cryptographic information reading step for reading, from a portable storage

6   medium, cryptographic information including information used to specify a certain part of the

7   content data on which cryptographic processing is to be performed;

8   a part specifying step for specifying the certain part of the ~~obtained~~ content data

9   based on the read cryptographic information <u>at least by searching for a specific data section in</u>

10   <u>the content data;</u>

11   a cryptographic processing step for encrypting the certain part; and

12   a content data recording step for recording the encrypted content data onto the

13   other storage medium.

1   59.   (Original) The program recording medium of Claim 58, wherein

2   the storage medium stores a plurality of pieces of content data as files, along with

3   cryptographic information for a plurality of file types corresponding to files that can be stored on

4   the storage medium; and

5   the cryptographic information reading step reads the cryptographic information

6   for a file type from the storage medium; and

7   the content data recording step records the encrypted content data onto the storage

8   medium as a file of the file type corresponding to the read cryptographic information.

1   60.   (Original) The program recording medium of Claim 58, wherein:

2   the cryptographic information includes bit pattern information showing a certain

3   bit sequence; and

4   the part specifying step detects, in the content data, bit data that matches the bit

5   sequence shown in the bit pattern information, and uses a location of the bit data as a basis for

6   specifying the certain part, the certain part having a fixed positional relationship to the bit data.

1   61.   (Original) The program recording medium of Claim 58 wherein:

2   the cryptographic information further includes at least one piece of algorithm

3   information for specifying an algorithm used for cryptographic processing; and

4   the cryptographic processing step performs encryption on the certain part using

5   the specified algorithm.

1   62.   (Currently Amended) A program recording medium storing a control program for

2   having a computer execute cryptographic processing on content data, the cryptographic

3   processing comprising:

4   a data obtaining step for obtaining, from received data, content data, and

5   cryptographic information including information used to specify a certain part of the content data

6   on which cryptographic processing is to be performed, the received data consisting of content

7   data and cryptographic information that has been multiplexed and transmitted;

8   a part specifying step for specifying the certain part of the obtained content data

9   based on the obtained cryptographic information at least by searching for a specific data section

10   in the obtained content data; and

11   a cryptographic processing step for performing one of encryption and decryption

12   on the certain part of the content data.

1   63.   (Original) The program recording medium of Claim 62, wherein:

2   the cryptographic information includes sync pattern information showing a certain

3   bit sequence; and

4   the part specifying step detects, in the content data, a sync pattern corresponding

5   to the bit sequence shown in the sync pattern information, and uses a location of the sync pattern

6   as a basis for specifying the certain part, the certain part having a fixed positional relationship to

7   the sync pattern.

1   64.   (Original) The program recording medium of Claim 63, wherein:

2   the part specifying step verifies the authenticity of the detected sync pattern by

3   checking whether another sync pattern is located at a position a set interval away from the

4   location of the detected sync pattern.

1   65.   (Original) The program recording medium of Claim 62, wherein:

2   the cryptographic information further includes at least one piece of algorithm

3   information for specifying an algorithm used for cryptographic processing; and

4   the cryptographic processing step performs one of encryption and decryption on

5   the certain part using the specified algorithm.

1   66.   (Currently Amended) A program recording medium storing a control program for

2   having a computer execute cryptographic processing on content data, the cryptographic

3   processing comprising:

4   a content data obtaining step for obtaining content data;

5   a cryptographic information obtaining step for obtaining cryptographic

6   information including information specifying a part on which cryptographic processing is to be

7   performed in the contents data, the information including a reference instruction indicating that a

8   data section in the content data be referred to;

9   a part specifying step for specifying the certain part of the content data based on

10   the cryptographic information by searching for and referring to the data section in the content

11   data as indicated by the reference instruction; and

12   a cryptographic processing step for performing one of encryption and decryption

13   on the certain part.

1   67.   (Original) The program recording medium of Claim 66, wherein:

2   the cryptographic information includes bit pattern information showing a certain

3 bit sequence; and

4   the part specifying step detects, in the content data, bit data that matches the bit

5 sequence shown in the bit pattern information, and uses a location of the bit data as a basis for

6 specifying the certain part, the certain part having a fixed positional relationship to the bit data.

1   68.   (Original) The program recording medium of Claim 67, wherein:

2   the indicated data section shows a length of the certain part; and

3   the part specifying step specifies the certain part of the content data by referring to

4 the data section as indicated by the reference instruction, and calculating the length of the certain

5 part based on the referenced data section.

1   69.   (Original) The program recording medium of Claim 66, wherein:

2   the cryptographic information further includes at least one piece of algorithm

3 information for specifying an algorithm used for cryptographic processing; and

4   the cryptographic processing step performs one of encryption and decryption on

5 the certain part using the specified algorithm.

1   70.   (Currently Amended) A portable data recording medium storing encrypted

2   content data, the data recording medium comprising:

3   a content data recording area in which content data, of which a certain part has

4   been encrypted, is recorded; and

5   a cryptographic information recording area in which cryptographic information,

6   including information used to specify the certain part of the content data <u>by searching for a</u>

7   <u>specific data section in the content data</u>, is recorded.

1   71.   (Original) The data recording medium of Claim 70, wherein:

2   each of a plurality of pieces of encrypted content data is recorded as a file in the

3   content data recording area; and

4   cryptographic information is recorded in the cryptographic information recording

5   area according to file type.

1   72.   (Original) The data recording medium of Claim 71, wherein:

2   the cryptographic information includes a reference instruction instructing a

3   decrypting apparatus decrypting the content data to refer to a data section in the content data.

1   73.   (Original) The data recording medium of Claim 72, wherein:

2   the cryptographic information includes bit pattern information showing a certain

3   bit sequence, and information instructing the decrypting apparatus to detect, in the content data,

4   bit data matching the certain bit sequence and use a location of the bit data as a basis for

5   specifying the certain part, the certain part having a fixed positional relationship to the bit data.

1   74.   (Original) The data recording medium of Claim 73, wherein

2   the indicated data section shows a length of the certain part; and

3   the part specifying step specifies the certain part of the content data by referring to

4   the data section as indicated by the reference instruction, and calculating the length of the certain

5   part based on the referenced data section.

1   75.   (Original) The data recording medium of Claim 71, wherein:

2   the cryptographic information further includes at least one piece of algorithm

3   information for specifying an algorithm used for cryptographic processing.

1   76.   (Original) The data recording medium of Claim 70, wherein:

2   the cryptographic information includes a reference instruction indicating to a

3   decryption apparatus decrypting the content data that a data section in the content data be

4   referred to.

1   77.   (Currently Amended) The data recording medium of Claim 76, wherein:

2   the cryptographic information further includes a detect instruction for detecting,

3   from the content data, bit data that matches the certain bit sequence shown by the bit pattern

4   information, and ~~specifies~~ ~~the decryption apparatus determines~~ the order in which the reference

5   and detect instructions are performed.

1   78.   (Original) The data recording medium of Claim 70, wherein:

2   the cryptographic information further includes at least one piece of algorithm

3   information specifying an algorithm to be used when decrypting the content data.

1   79.   (Original) The data recording medium of Claim 78, wherein:

2   the cryptographic information includes .a plurality of pieces of algorithm

3 information and pieces of range information showing the application range of each piece of

4 algorithm information.

1   80.   (Original) The data recording medium of Claim 79, wherein:

2   the cryptographic information includes priority ratings used to determine which

3 algorithm information should be applied when the application ranges of a plurality of pieces of

4 algorithm information overlap.

1   81.   (Currently Amended) A cryptographic processing method, comprising:

2   a data reading step for reading content data and cryptographic information from a

3 portable storage medium, the cryptographic information including information used to specify a

4 certain part of the content data on which cryptographic processing is to be performed;

5   a part specifying step for specifying, based on the read cryptographic information,

6 the certain part of the read content data <u>at least by searching for a specific data section in the read</u>

7 <u>content data</u>; and

8   a cryptographic processing step for performing one of encryption and decryption

9 on the certain part of the read content data.

1   82.   (Currently Amended) A cryptographic processing method encrypting content

2   data and recording the encrypted content data onto a storage medium, the cryptographic

3   processing method comprising:

4   a cryptographic information reading step for reading, from a portable storage

5   medium, cryptographic information including information used to specify a certain part of the

6   content data on which cryptographic processing is to be performed;

7   a part specifying step for specifying the certain part of the ~~obtained~~ content data

8   based on the read cryptographic information <u>at least by searching for a specific data section in</u>

9   <u>the content data</u>;

10   a cryptographic processing step for encrypting the certain part; and

11   a content data recording step for recording the encrypted content data onto the

12   storage medium.

1   83.   (Currently Amended) A cryptographic processing method performing

2   cryptographic processing on content data, the cryptographic method comprising:

3   a data obtaining step for obtaining, from received data, content data, and

4   cryptographic information including information used to specify a certain part of the content data

5   on which cryptographic processing is to be performed, the received data consisting of content

6   data and cryptographic information that has been multiplexed and transmitted;

7   a part specifying step for specifying the certain part of the obtained content data

8   based on the obtained cryptographic information <u>at least by searching for a specific data section</u>

9   <u>in the obtained content data</u>; and

10   a cryptographic processing step for performing one of encryption, and decryption

11 on the certain part of the content data.

1   84.   (Currently   Amended) A   cryptographic   processing   method   performing

2 cryptographic processing on content data, the cryptographic processing method comprising:

3   a content data obtaining step for obtaining content data;

4   a cryptographic information obtaining step for obtaining cryptographic

5 information including information specifying a part on which cryptographic processing is to be

6 performed in the contents data, the information including a reference instruction indicating that a

7 data section in the content data be referred to;

8   a part specifying step for specifying the certain part of the content data based on

9 the cryptographic information by <u>searching for and</u> referring to the data section in the content

10 data as indicated by the reference instruction; and

11   a cryptographic processing step for performing one of encryption and decryption

12 on the certain part.

1   85.   (New) A cryptographic apparatus comprising:

2   a data reading means for reading content data and cryptographic information from

3 a portable storage medium, the cryptographic information including information used to specify

4 a certain part of the content data on which cryptographic processing is to be performed;

5   a part specifying means for specifying, based on the read cryptographic

6 information, the certain part of the read content data; and

7   a cryptographic processing means for performing one of encryption and

8 decryption on the certain part of the read content data, wherein:

9   the cryptographic information further includes a plurality of pieces of algorithm

10   information for specifying an algorithm used for cryptographic processing, pieces of range

11   information each showing a range over which an algorithm is applied, and information showing

12   priority ratings indicating an order in which the pieces of algorithm information should be

13   applied;

14   the cryptographic processing means selects, for each application range in the

15   certain part, a piece of algorithm information based on the range information, and uses an

16   algorithm specified by the piece of algorithm information to perform one of encryption and

17   decryption on the application range; and

18   when the application ranges of a plurality of algorithms overlap, the cryptographic

19   processing means selects pieces of algorithm information according to the priority ratings.

1   86.   (New) A cryptographic apparatus encrypting content data and recording the

2   encrypted data onto a storage medium, the cryptographic apparatus comprising:

3   a content data obtaining means for obtaining content data;

4   a cryptographic information reading means for reading, from a portable storage

5   medium, cryptographic information including information used to specify a

6   certain part of the content data on which cryptographic processing is to be performed;

7   a part specifying means for specifying the certain part of the obtained content data

8   based on the read cryptographic information;

9   a cryptographic processing means for encrypting the certain part; and

10   a content data recording means for recording the encrypted content data onto the

11   storage medium, wherein:

12   the cryptographic information further includes a plurality of pieces of algorithm

13   information for specifying an algorithm used for cryptographic processing, pieces of range

14   information each showing a range in the content data over which an algorithm is applied, and

15   information showing priority ratings indicating an order in which the pieces of algorithm

16   information should be applied;

17   the cryptographic processing means selects, for each application range in the

18   certain part, a piece of algorithm information based on the range information, and uses an

19   algorithm specified by the piece of algorithm information to encrypt data in the application

20   range; and

21   when the application ranges of a plurality of algorithms overlap, the cryptographic

22   processing means selects pieces of algorithm information according to the priority ratings.

1   87.   (New) A cryptographic apparatus comprising:

2   a data obtaining means for obtaining, from received data, content data, and

3   cryptographic information including information used to specify a certain part of the content data

4   on which cryptographic processing is to be performed, the received data consisting of content

5   data and cryptographic information that has been multiplexed and transmitted;

6   a part specifying means for specifying the certain part of the obtained content data

7   based on the obtained cryptographic information; and

8   a cryptographic processing means for performing one of encryption and

9   decryption on the certain part of the content data, wherein:

10   the cryptographic information further includes a plurality of pieces of algorithm

11   information for specifying an algorithm used for cryptographic processing, pieces of range

12   information each showing a range over which an algorithm is applied, and information showing

13   priority ratings indicating an order in which the pieces of algorithm information should be

14   applied;

15   the cryptographic processing means selects, for each application range in the

16   certain part, a piece of algorithm information based on the range information, and uses an

17   algorithm specified by the piece of algorithm information to perform one of encryption and

18   decryption on the application range; and

19   when the application ranges of a plurality of algorithms overlap, the cryptographic

20   processing means selects pieces of algorithm information according to the priority ratings.

1   88.   (New) A cryptographic apparatus performing cryptographic processing on

2   content data, the cryptographic apparatus comprising:

3   a content data obtaining means for obtaining content data;

4   a cryptographic information obtaining means for obtaining cryptographic

5   information including information specifying a part on which cryptographic processing is to be

6   performed in the contents data, the information including a reference instruction indicating that a

7   data section in the content data be referred to;

8   a part specifying means for specifying the certain part of the content data based on

9   the cryptographic information by referring to the data section in the content data as indicated by

10   the reference instruction; and

11   a cryptographic processing means for performing one of encryption and

12   decryption on the certain part, wherein:

13   the cryptographic information further includes a plurality of pieces of algorithm

14   information for specifying an algorithm used for cryptographic processing, pieces of range

15   information each showing a range over which an algorithm is applied, and information showing

16   priority ratings indicating an order in which the pieces of algorithm information should be

17   applied;

18   the cryptographic processing means selects, for each application range in the

19   certain part, a piece of algorithm information based on the range information, and uses an

20   algorithm specified by the piece of algorithm information to perform one of encryption and

21   decryption on the application range; and

22   when the application ranges of a plurality of algorithms overlap, the cryptographic

23   processing means selects pieces of algorithm information according to the priority ratings.

1   89.   (New) A portable data recording medium storing encrypted content data, the data

2   recording medium comprising:

3   a content data recording area in which content data, of which a certain part has

4   been encrypted, is recorded; and

5   a cryptographic information recording area in which cryptographic information,

6   including information used to specify the certain part of the content data, is recorded, wherein:

7   the cryptographic information further includes a plurality of pieces of algorithm

8   information for specifying an algorithm to be used when decrypting the content data, pieces of

9   range information showing the application range of each piece of algorithm information, and

10   priority ratings used to determine which algorithm information should be applied when the

11   application ranges of a plurality of pieces of algorithm information overlap.